Deloitte.

Risk powers performance

Navigating the major risk trends in Energy, Resources & Industrials for competitive advantage

A new view of risk management

Risk is often seen as something to be mitigated and managed in order to protect against loss.

At Deloitte, we believe risk management can be a value-creating activity. We help businesses gain a new view of risk—seeing risk management as a vital performance lever that can reveal untapped opportunities to create competitive advantage.

Today's business climate is characterized by disruption and volatility. The companies that thrive are those that identify the major drivers of change that affect risk and exploit them more effectively than their peers.

Risk trends:

Industrial controls: Too much at stake to ignore 04

Getting a grip on the extended enterprise 05

Cyber everywhere! 06

Third-party risk management: A source of strategic advantage 08

A revitalized view of risk through integrated assurance 09

Product security: It starts with the manufacturer 10

Turning digital risk into digital advantage 12

Treasury and cash management in a complex global organization 13

Sustainability: Creating value through lowering carbon emissions 14

Energy trading: Optimizing the hydrocarbon value chain 16

Four catalysts for transformation

Four global drivers have served as catalysts for transformation in the business and operations of Energy, Resources & Industrials (ER&I) companies.

1. Regulatory scrutiny

Heavy industry and critical infrastructure attract special attention from regulators because of the potential impact on communities and the environment. Awareness is high among citizens and information can be spread around the world in an instant. Lawmakers are responding with increasingly stringent regulations and expectations for best practices in socially responsible, sustainable operations.

Companies must meet the demands of the complex regulatory landscape, but be flexible enough that the regulatory program keeps pace with a rapidly changing environment—all with an industry focus.

Is your approach to regulatory risk designed to preserve value and power performance?

2. Digital transformation

New technologies can transform industrial processes. Automation, connectivity, artificial intelligence and advanced analytics are driving efficiencies and optimization as well as closer supply chain integration. Unfortunately, these trends can also expose companies to potential misuse of information and interruption of critical activities.

Today's business environment is global and highly interconnected, increasing the probability of cyber threats. In an era of complexity, when cyber is everywhere, effective cyber risk management will give organizations the confidence to take full advantage of technological opportunities.

Are you prepared to take advantage of the promise of digital while avoiding the pitfalls?

3. Safety and reliability

Many industrial processes are inherently risky. As operational scale and complexity increase, automation replaces human supervision, and external suppliers play an ever-greater role, the potential for unintended safety outcomes can increase. The tolerance of customers and the broader community for missteps is decreasing, placing organizations at greater risk, and increasing stakeholder scrutiny of their operations.

Does your company make safety and reliability a top priority in times of rapid change?

4. Sustainability

More and more, consumers, investors and other stakeholders are asking organizations to use cleaner, more carbon-neutral forms of energy—marking a global shift away from traditional forms of energy. In response, as they think about how they produce and extract their products, organizations need to plan for a low-carbon economy. Together, these drivers are both heightening risks and creating significant opportunities.

Is your company driving value creation through sustainable practices?

In this document, we explore 10 specific risk trends for which ER&I companies need to prepare.

Industrial controls: Too much at stake to ignore

The ER&I industry has undergone a transformation in the way it operates large-scale industrial and infrastructure processes. The vast majority of operational technology (OT) is now automated, with actions driven by algorithms or sensors. Systems that were not previously considered to be at risk from external threats are now virtually all connected to networks.

Connected OT offers tremendous benefits, including reduced costs, improved safety, higher reliability and the ability to optimize processes. But it has also exposed the enterprise to a whole new array of risks.

The risks of operating critical infrastructure

The critical infrastructure and economic significance of ER&I make it an attractive target for cyber-attacks. Threat actors can range from low-level cyber criminals and "hacktivists" to sophisticated criminal syndicates and nation-states.

The consequences of a successful attack can be catastrophic. A billion-dollar asset could be lost. Production could be taken offline for months, with significant financial impact. A facility could be shut down suddenly, and damaged or destroyed as a result, with implications for safety and the environment. If the facility is providing essential services like power, water or transportation, the effects can cascade throughout society.

Companies need to ask themselves some important questions:

- Have we identified the potential risks of digitizing our OT? Organizations are often quick to adopt new technologies, eager to capture the gains.
- Have we measured the risk and compared it to our overall risk appetite?
- Do we have effective industrial controls in place?

Best practice

Industrial control risks are similar to cybersecurity risks; however, organizations cannot simply apply IT security principles to their industrial assets. OT is typically installed and maintained by engineering staff, while IT teams manage enterprise cybersecurity. These groups have not traditionally worked closely or harmoniously together within large companies.

The best outcomes occur when companies rationalize security over both operational systems and IT systems. A multidisciplinary approach brings all the skill sets together to find the best solution. Ideally, an organization's IT team and engineering staff adopt a common approach to securing company assets.

The NotPetya ransomware attack in 2017 caused total damages estimated at more than US$10 billion worldwide. Costs reached the hundreds of millions for several organizations, including a large confectionary company, a well-known package delivery service and a major shipping container company.[1]

Getting a grip on the extended enterprise

ER&I companies are increasingly relying on suppliers to perform core functions and manage key parts of their business. Complex and large-scale operating models may encompass multiple contractors working within an organization's own facilities or on its property. Direct suppliers may, in turn, contract work out to sub-contractors of their own. This multi-tiered network of suppliers is called the "extended enterprise."

Potential risks: Control, increased costs, and much more

Despite their close integration, suppliers are often being inadequately monitored to verify that they are meeting performance standards, following safety and regulatory protocols, and complying with contract terms. Companies may neglect to apply the same high standard of controls over the subcontractors that they implement for their own internal operations.

In addition to the issue of not holding contractors and sub-contractors to the same high standards, there is also the potential risk that companies may be overpaying for services received, resulting in significant value leakage over the life of a contract. The leakage is often the result of poorly understood contract terms or infrequent compliance reviews. Companies may not be collecting the right information from their suppliers, or may fail to review the information in a timely manner. The financial impact can be significant, typically reaching one to five percent of the value of contracts.

The risks go beyond costs and controls. Project timelines could be jeopardized. Cybersecurity could be breached through the vulnerabilities of a supplier. The likelihood of health and safety or environmental incidents may increase.

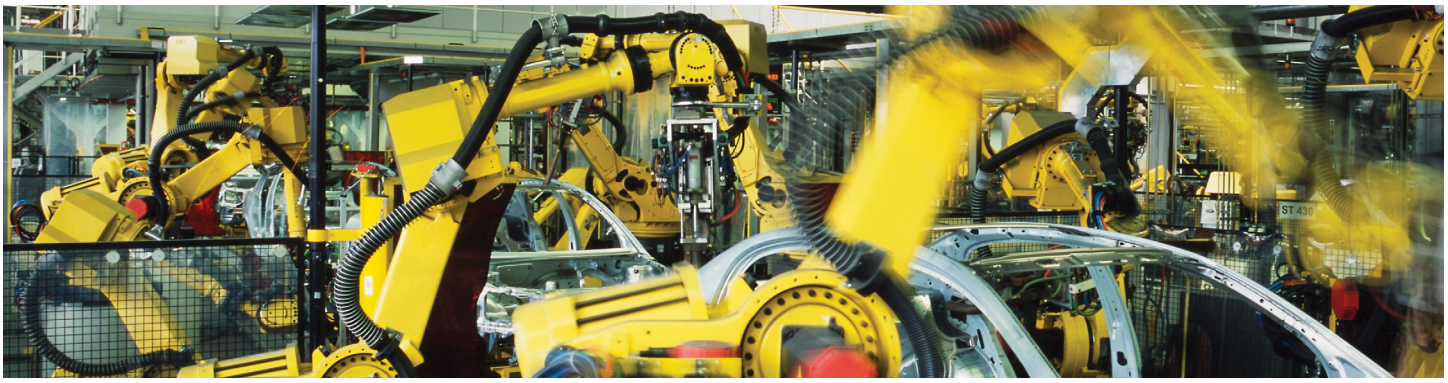
In the event of a high-profile event like a fatality or a spill, external stakeholders will not distinguish between a third-party supplier and the company itself. The potential damage to brand and reputation must be taken into account.

Best practice

The best approach to Extended Enterprise Risk Management (EERM) is a proactive one that offers a 360-degree view of suppliers. An emerging practice in EERM is to implement real-time monitoring so that any issues can be identified and addressed as they arise.

Cyber everywhere!

ER&I companies are adopting digital technology at a more rapid pace than ever before. Examples of technology adoption include digital oil fields, human-less mines and fully automated factories. The digitization of services and processes has made highly sensitive data available to consumers and workers alike through their mobile devices—anytime and anywhere.



While this increased connectivity has benefits, it has also expanded the volume and probability of cyber-attacks around the world. Threat actors have embraced the expanded digital footprint and are becoming increasingly sophisticated about taking advantage of vulnerabilities. Within the ER&I industry, cybersecurity is expected to be one of the biggest areas of spending growth.

Cybersecurity challenges

The ER&I industry faces several cybersecurity challenges:

- Some segments of the ER&I industry have historically been under-regulated in cybersecurity and have not invested as much in this area as other industries.
- With demand for skilled cybersecurity professionals outpacing supply, ER&I can be at a disadvantage when competing for talent with better-known companies and consumer brands perceived to be at the forefront of technology.
- Industrial control systems (ICS) infrastructure has a different operating profile and longer life span than IT equipment, making it more challenging to address specific cyber threats to the equipment that runs ER&I.
- Cybersecurity stretches across all aspects of an ER&I company's business, and cyber threats merge with physical security, safety, fraud and risk management. The challenge is magnified when the company is operating critical infrastructure. This creates complex governance challenges that can leave gaps in controls and oversight.

Trends adding to the risks

A number of trends are leading to increased cybersecurity risk for ER&I companies:

- The entire operating environment is becoming more digitized. There has been a massive proliferation of devices that need to be managed. IoT networks are connecting to legacy infrastructure that had no need for security protection in the past. Cybersecurity must reach every last endpoint.
- Attacks often start with a compromised digital identity somewhere in the system. Identities were once assigned largely to employees with passwords, but now all connected devices and operational technology have their own identities. They must all be considered untrusted until they have been authenticated.
- Increasing interconnectedness with third-party suppliers exposes companies to potential vulnerabilities wherever a supplier lacks adequate cybersecurity.

Best practice

While cybersecurity risks and challenges are numerous, an effective cyber risk management strategy enables organizations to build the confidence that allows them to take advantage of every technological opportunity that arises. To achieve effective cyber risk management, it is essential that organizations redefine their perception of cyber risk—assessing and discussing the larger role cyber plays in empowering the company. Cybersecurity should not be viewed as a high-risk component of the business, but as an enabler for new opportunities.

Organizations need to understand the full scope of their cyber footprint, getting visibility into what all the devices are and then establishing appropriate governance and continuous real-time monitoring.

Ownership of cybersecurity within organizations should be clear, clarifying who is responsible for policy-setting and implementation.

Third-party risk management: A source of strategic advantage

Any third party that contracts directly with an organization has the potential to become a "weak link" that affects security, reputation or performance. The scale of third-party relationships is enormous for ER&I companies. Systematic lapses—such as mismanagement of billings or contracts—can add up to material cost impacts. Companies are therefore always seeking ways to manage third-party risks in a more efficient manner.

New ways of thinking about third-party risk

ER&I companies are broadening their concept of third-party risks in a number of ways:

- **Types of third parties:** ER&I companies have traditionally focused mainly on vendors, and therefore put a lot of rigor into evaluating risks during the procurement process. Today, they are looking more carefully at others as well.
- **Types of risk:** Oil & Gas and Mining companies were historically concerned with two main types of risk: health and safety, and anti-bribery and corruption. Today, they consider a much broader range of risks, including cyber security, data privacy, labor rights and sustainability.
- **Use of technology:** New technology solutions, as well as new functionality on existing platforms, are emerging as viable tools to manage third-party risks.
- **Industry cooperation:** Companies within the ER&I industry are beginning to cooperate through initiatives where they collectively perform risk assessments on the suppliers many of them share.

Responsible supply chain

In today's climate of increasing regulation and cross-border enforcement, legal and reputational liability can be passed from supplier to purchaser. Data privacy, labor requirements, anti-bribery, modern slavery and sanctions regulations are but a few of the regulatory and ethical considerations that must be effectively managed by a global enterprise.

As expectations increase around ethical behavior, regulatory compliance in the supply chain is no longer sufficient. Demonstrable, proactive and systematic management of ethical and environmental topics is increasingly seen as business-critical; companies must establish a social license to operate alongside regulatory compliance.

Companies are increasingly being held accountable for topics related to climate change and sustainability. There is an expectation that they will hold third parties to the same requirements and standards to allow for a responsible supply chain before their products reach consumers or other businesses.

Best practice

Many companies are taking a more holistic and integrated approach, bringing all third-party risk management activities together under one ownership structure.

Important elements of effective risk management include: overall governance structure; clear policies and standards; detailed processes and standards; training and education; and a review of the supply chain from an ethically responsible perspective.

83 percent of organizations experienced a third-party incident in the past three years.[2]

11% severe impact

35% moderate impact

A revitalized view of risk through integrated assurance

High-profile risk events and regulatory changes have proliferated over the past decade. In response, ER&I companies have placed a high priority on risk oversight and devoted significant resources to assurance programs.

The core purpose of assurance activities is to provide confidence to the leadership team that the organization is managing its risks and reaching its objectives.

Too much information, not enough insight

Increased spending on assurance programs has not always delivered the intended results. Many companies recognize that they are performing a lot of uncoordinated assurance, at significant direct and indirect cost, for too little benefit. These organizations have characterized their assurance activities as narrowly focused, redundant, costly, intrusive to the business, and unrelated to drivers of value and performance. As a result, boards lack a clear, accurate and comprehensive picture of the greatest risks facing the company.

An integrated assurance model

Companies seeking better outcomes are increasingly turning to integrated assurance. They are simplifying and standardizing the assurance model in order to refocus on its core purpose.

Integrated assurance is the coordinated planning, execution and reporting of assurance activity under a common governance model. This approach not only aims to rationalize assurance and achieve efficiencies, it also directs assurance activities to where they will create the most value for the organization.

The foundation of an integrated assurance model is the identification of key drivers of value in the business, so that assurance activities are aligned with critical objectives. For ER&I companies, value drivers often include five pillars: safety, operational integrity, asset performance, financial resiliency and production growth.

Best practice

For integrated assurance to be successful, a single and senior role should be accountable for assurance organization-wide. This should lead to three important results:

1. A focus on the activities that really impact business outcomes.
2. A reduced burden on the business.
3. Coordination, leading to better planning, enhanced capability and consistent reporting.

The six layers model

Product security: It starts with the manufacturer

Many consumer products now incorporate the ability to connect to networks, applications and nearby devices. Connectivity enhances the products' functionality, but it also adds significant cyber risks and potential points of entry for threat actors. In the environment of Industry 4.0, disruptive technologies and trends—such as the Internet of Things, robotics, virtual reality and artificial intelligence—are changing the way we live and work.

While end users share responsibility for managing risks, the manufacturers of these products must ensure they design security features and controls ("security by design") into their devices so that they can defend against the type of cyber-attacks we are seeing today—and what we might see tomorrow.

Industrial applications
ER&I companies use connected devices organization-wide. Examples include advanced technologies like robotics, sensors, programmable logic controllers and digital twins.

Traditional products like heating, ventilation, and air conditioning (HVAC) distribution control systems (DCS) and building controls systems (BCS) are increasingly connected to networks.

These devices form part of the operational technology, data collection and analytics systems that help deliver more efficient, effective manufacturing capability that is needed to manufacture products. Given the connectivity of all these devices, manufacturers are increasingly seeing a need for product security to be top of mind for ER&I R&D, supply chain management, product developers and risk managers.

Consumer applications
Connected products can include home appliances, entertainment devices, smart speakers, wearable technology, medical devices and equipment, and automobiles.

A security breach could expose an individual's private communications or images, medical information, location and other personal details. A cyber-attack against these consumer devices could result in physical harm to the consumer (e.g., medical device cyber-attacks or connected vehicle cyber-attacks).

Product security challenges
Many older Internet of Things (IoT) devices lack robust security protocols and industrial-strength encryption capable of protecting data-at-rest and data-in-motion. IoT products often contain back doors and software flaws that make them easy to hack.

Devices may have a lifespan of five to 20 years, throughout which the risk of attacks can grow, as the vulnerabilities in the unpatched operating systems and firmware are well known to the hacking community. Even actions taken to improve security, such as patch updates, can create new risks.

There are no overarching standards for how the different parts of an IoT stack should interact. Different vendors and industries use their own standards, which may be incompatible.

In a competitive market, many buyers do not wish to pay higher prices for greater product security.

Best practice
Manufacturers need to consider product security from the outset and "design" it into their products. For example, they may build in encrypted communication paths, authentication protocols and access controls. Security must be considered just as essential as a product's functionality and marketability.

Even after products are sold, manufacturers must be prepared to track them, and monitor for new types of attacks and threat vectors so that they can fully support their customers.

Companies need to have a clear understanding of what product security is, and where it should live within the organization.

In 2013, hackers used internet-enabled heating, ventilation and air-conditioning systems set up in a chain of retail stores to steal 40 million credit card numbers.[3]

Turning digital risk into digital advantage

ER&I companies are rapidly transitioning to digital technologies such as robotics, artificial intelligence (AI), machine learning, Internet of Things (IoT), digital consumer interfaces and cloud storage of data. Digitization offers tremendous potential benefits, including improved efficiency, faster production cycles and better analytics.

Companies must be confident in embracing these innovations—they have little choice if they wish to remain competitive. It is important that they create a trusted ecosystem to leverage new technologies while effectively managing the risks.

Two types of digital risk

Digital risks fall under two main categories:

- **The risks of transforming to digital.** Compared to other capital investments, there is more uncertainty about whether digital technologies will deliver on expected benefits. Implementation is often managed by smaller or non-traditional vendors and delivery partners. Integration with the legacy environment can be a challenge.
- **Controlling digital risks post-transformation.** Companies must manage privacy concerns, regulatory issues, security and issues particular to the technologies themselves, such as an inherent bias associated with AI.

The challenges of digitalization

ER&I companies have traditionally dealt with risks that are well understood and foreseeable, with proven mitigation strategies. In contrast, digital risk can emerge as a pressing issue within hours or minutes, instead of weeks or months. The technology is so new that the risks are still being uncovered and effective controls are still being developed.

Digital technology is encouraging some industrial companies to change their business model. B2B companies are bypassing traditional channels and becoming B2C, and the end customer is often interacting directly with a technology rather than a person. Similarly, social media is creating new expectations for responding to the public, with implications for brand and reputation.

Many organizations lack the skill sets required to manage digital risks. Because these systems are so new, there is a limited history of implementing them and a limited pool of knowledge upon which to draw. This compounds the difficulty of identifying the risk profile of new technologies and understanding how to react.

Best practice

Digital risk management seeks to establish proper governance around digital technologies. Traditional assurance models are generally not effective, and many companies are transforming their enterprise risk models to account for the risks that digitization brings to business operations. Companies must be very adaptable to keep pace in this ever-changing, agile and consumer-centric world.

Effective practices may include a thorough scenario analysis, pre-implementation risk identification and strategy, authorization and testing protocols, increased training, the establishment of specific parameters (e.g., no system shall rely on a single sensor), and ongoing monitoring and testing.

Treasury and cash management in a complex global organization

Most ER&I companies have operations spanning multiple countries. They must maintain sufficient cash resources within each jurisdiction to make investments and to support the day-to-day needs of the business.

The core responsibilities of treasury departments are to manage liquidity, funding and market exposures. Their success is driven by their ability to navigate external factors, including foreign exchange rates, interest rates and commodity prices. Each of these factors introduces its own set of risks with the potential to materially affect a company's reported financial results.

The trend toward thinner margins in the ER&I industry increases the pressure to manage cash resources more efficiently and strive for working capital optimization.

The challenges of multinational operations

Foreign currency risk is a top concern for many ER&I companies. Exchange rates reflect continual changes in macroeconomic conditions and government policies, as well as geopolitical factors that can be difficult to predict. The risk is magnified for companies producing commodities that trade in a different currency than the ones in which they incur the majority of their costs.

Operating in certain developing countries carries additional challenges. There may be restrictions on moving funds in or out of the country. Regulations may prohibit currency hedging. The local banking infrastructure may be inadequate to support the needs of large companies.

In a world of constant change, many treasury professionals also need to consider how treasury plays a part in the strategic, operational and compliance-related risks of the organization. Incorporating treasury risk management principles into the wider enterprise risk management structures will bring a more holistic approach—one that can have significant benefits for an organization's bottom line.

Best practice

Companies have long relied on methods like hedging and detailed manual forecasts to manage treasury risks. These methods are becoming less effective as operational complexity increases.

Emerging tools such as cloud-based treasury management systems can reduce operating costs, help manage risk, create better visibility and improved reporting capabilities, and enable better governance and decision management.

Cash concentration structures and in-house banks offer another interesting solution. They can provide access and visibility to global cash balances in a single location, allowing a company to pool all its cash together, settle intra-company transactions and make decisions for the business as a whole.

Sustainability: Creating value through lowering carbon emissions

Reducing greenhouse gas emissions, transitioning to cleaner forms of energy, mitigating climate risk and meeting the energy needs of today while preparing for the changing needs of tomorrow are some of the most important risks in the broader category of social and environmental sustainability. If not incorporated into an organization's sustainability strategy, these risks have the potential to disrupt the value chain of every business on the planet.

The impact of these risks on ER&I companies includes, but is not limited to, damage to their facilities from extreme weather events, litigation and penalties for not meeting regulations, potential supply chain interruptions of critical goods and services, increased insurance costs, difficulty recruiting employees and poor stakeholder relations.

Stakeholders expectations have increased

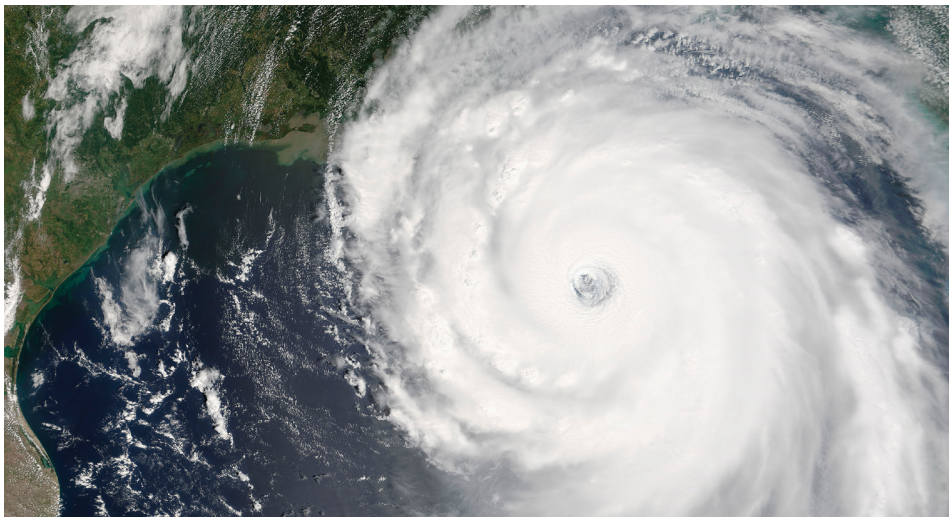
The conversation has radically shifted. Stakeholders are no longer satisfied with supportive statements or high-level policies on sustainability. Instead, they want specifics on how the organization is shifting toward a sustainable business model—while implementing actions to prevent stranded assets and ensure that investors' capital is being well managed. Companies that are unable to offer well-thought-out sustainability plans will be unprepared for these conversations.

For large public companies, initiatives like the Task Force on Climate-Related Financial Disclosures (TCFD) are changing disclosure expectations. Companies must demonstrate that they have identified both climate-related risks and opportunities, and that they have processes in place to manage those risks on an ongoing basis.

Going to the heart of corporate strategy

Climate risk affects corporate strategy in a fundamental way, and traditional business models should be reassessed by asking a few key questions:

- Where are the vulnerabilities in our supply chain?
- Do we have key assets located in vulnerable regions? How resilient are we to potential changes over time?
- How will our business, and the way we do business, change based on the imperatives that being a sustainable organization will force?
- If sustainability will be driving our future, what would we like that future to look like?



Best practice

Effective management of a sustainability strategy requires organizations to address it in multiple ways:

- Establish clear ownership of sustainability at the executive and board level.
- Build sustainability stress testing into the core corporate strategy.
- Establish clear metrics and targets that address risks and opportunities. For example, quantify and set a goal for reducing exposure to climate risk, and specify timelines for taking advantage of opportunities. Targets should be shared publicly with key stakeholders.
- Review different scenarios, such as potential regulatory changes or market-based mechanisms, and evaluate the company's resilience.
- Leverage the power of digital, analytics and AI to understand the organization's environmental impact and emission trends, and how it can be more efficient.
- Drive value through sustainability efforts such as switching to renewable energy sources, or trading in "green energy" credits.

With new sources of energy becoming cheaper and more readily available, companies need to contemplate how they produce and extract their product.

US$23 trillion

of global investments were guided by environmental, social and governance (ESG) criteria in 2017.

In the US, ESG investments totaled

US$12 trillion

or one-quarter of all investment dollars.[4]

Energy trading: Optimizing the energy value chain

After decades of relative consistency, the nature of energy trading has changed in recent years. There has been an evolution in the parties transacting and the information available to guide their decisions.

Evolving parties
Speculative traders and financial institutions are much less active in energy transactions than in years past. A greater proportion of trading is now carried out by energy industry participants whose goal is to optimize the value of their own assets. Pricing, therefore, better reflects the fundamentals of supply and demand. Furthermore, energy producers are increasingly marketing further downstream—for example, directly to refineries—in an effort to increase their margins.

Advancing technology
Some of the most disruptive influences on energy trading are new technologies:

- **Digitization**, such as sensors on pipelines and digital record-keeping, has exponentially increased the amount of data available for analysis and use in decision-making.
- **Optimization engines** powered by AI are being developed to apply product supply chain principles to the hydrocarbon value chain.
- Sophisticated **data science, analytics and processing techniques** are enabling some companies to develop a clearer picture of market dynamics.
- We are beginning to see **digital trade floors** that combine blockchain, chatbots and other technologies to create efficiencies in trading, dramatically shorten payment cycles and reduce the working capital tied up in receivables.
- Niche trading platforms—or in some cases, basic spreadsheets—are being overtaken by **consolidated platforms** offering endless processing power and on-demand risk and position reporting.

Constrained supply
In addition to traditional risks like geopolitical factors, we are seeing new restraints imposed on supply. Public pressure and regulatory actions can lead to the delay or even cancellation of major projects. For example, some governments have curtailed pipeline development due to environmental concerns, and transportation capacity constraints can impact pricing in a particular market segment.

In a volatile market, it is challenging to make effective hedging and trading decisions if one's counterparties have superior analytical tools and information. As many energy companies have learned, the impact of poor trading decisions is hedging losses, foregone revenue opportunities and volatility in reported financial results.

Best practice
ER&I companies must ensure they have effective governance processes in place, including organizational structure, and risk policies and procedures. The overall controls framework needs to be reviewed for new digital risks.

Companies need a technology infrastructure that allows them to see their worldwide long and short positions and exposures on a near-real-time basis and react to volatility in the marketplace.

The path forward with Deloitte

It is time for ER&I companies to take a more holistic, opportunistic look at risk. New market dynamics, such as digital technologies and globalization, have created new risks. By understanding risk more precisely at every level of the organization, businesses can exploit these new market dynamics more effectively than their competitors, creating a distinct advantage.

Leading organizations take calculated risks, with new products, new markets and acquisitions. At the same time, disruptors can threaten even the greatest business strategy as well as your brand.

Deloitte's approach to risk management

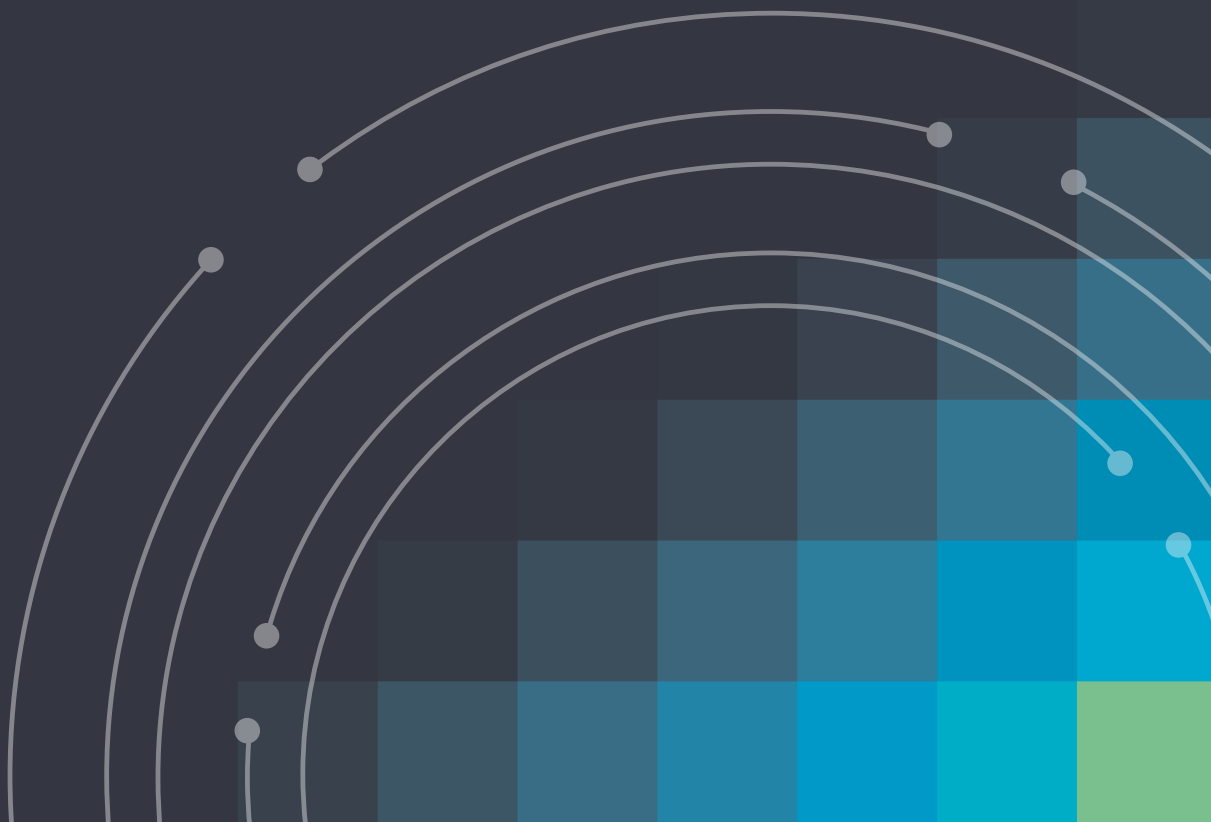
As a leading global Risk Advisory practice, our approach can simultaneously deliver value creation and value protection for our clients. We help business leaders exploit superior risk management practices to create competitive advantage.

Deloitte enables organizations to make risk-informed strategic choices and respond to disruptions to grow their business and protect their reputation. We help the C-suite and board of directors have the right insights, best-in-class corporate governance and a risk culture aimed at driving value.

A unique cross-functional team

The Deloitte team has unparalleled expertise and on-the-ground experience in industry. We are active in every region of the globe. Our consultants include field engineers, asset reliability experts and digital scientists. These diverse backgrounds enable us to deploy the best resources, quickly understand clients' issues and identify the most appropriate tailor-made solutions.

We would welcome the opportunity to help your organization gain a new view of risk.



Endnotes

1. Source is the following article from Wired.https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
2. Source is the Deloitte press release that can be found at..https://www2.deloitte.com/uk/en/pages/press-releases/articles/over-eight-in-ten-organisations-experience-third-party-failure.html
3. Source is a Deloitte report found at the link below. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Internet-of-Things-Innovation-Report-2018-Deloitte.pdf
4. Source: Sustainability: Drivers for Change (Deloitte slide presentation)

Notes

Contact us:

Paul Zonneveld
Partner
Clients & Industries Lead
+1 403 617 5777
pzonneveld@deloitte.ca

Rene Waslo
Partner
Cybersecurity
+1 412 400 1638
rwaslo@deloitte.com

Sean Peasley
Partner
Industrial Controls
+1 714 334 6600
speasley@deloitte.com

Russell Jones
Partner
Product Security
+1 415 248 6032
rujones@deloitte.com

Emily Cromwell
Director
Digital Risk, Third Party Risk
+44 75 5720 4377
ecromwell@deloitte.co.uk

Charlotte Gribben
Partner
Digital Risk
+44 77 3621 2539
cgribben@deloitte.co.uk

Mark Bethell
Partner
Third Party Risk
+44 79 1718 3787
mabethell@deloitte.co.uk

Henry Stoch
Partner
Sustainability
+1 604 761 1780
hstoch@deloitte.ca

Prashant Patri
Partner
Treasury and Cash Management
+1 347 331 5653
prpatri@deloitte.com

Trent Gall
Partner
Energy Trading and
Risk Management
+1 403 830 9016
tgall@deloitte.ca

Munir Patel
Partner
Integrated Assurance
+1 587 777 4407
munirpatel@deloitte.ca

Laura Joudrie
Partner
Extended Enterprise
Risk Management
+1 416 775 7020
ljoudrie@deloitte.ca

Deloitte.

www.deloitte.com